Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 14 mars 2012
N° CERTA-2012-AVI-138

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Remote Desktop Protocol

Gestion du document

Référence	CERTA-2012-AVI-138
Titre	Multiples vulnérabilités dans Remote Desktop Protocol
Date de la première version	14 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-020 du 13 mars 2012
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Windows XP SP3 ;
- Windows XP Professional édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 édition x64 Service Pack 2 ;
- Windows Server 2003 SP2 pour systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 et 64 bits ;
- Windows 7 pour systèmes 32 et 64 bits Service Pack 1 ;
- Windows Server 2008 R2 ;

- Windows Server 2008 R2 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium ;
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

3 Résumé

Deux vulnérabilités ont été corrigées dans *Remote Desktop Protocol* (ou « RDP »). La plus critique permet l'exécution de code arbitraire à distance.

4 Description

Deux vulnérabilités ont été corrigées dans RDP. La première permet à un attaquant d'exécuter du code arbitraire à distance au moyen d'une séquence de paquets spécialement conçus (CVE-2012-0002). La seconde permet à un attaquant de réaliser un déni de service à distance en bloquant le service RDP visé (CVE-2012-0152).

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS12-020 du 13 mars 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-020
  http://technet.microsoft.com/en-us/security/bulletin/MS12-020
- Référence CVE CVE-2012-0002 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
- Référence CVE CVE-2012-0152 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152

Gestion détaillée du document

14 mars 2012 version initiale.